



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/698,159	10/30/2000	Anup K. Ghosh	CIG-103	7526

7590 05/12/2005

Brett C. Martin  
1650 Tyson Blvd.  
McLean, VA 22102

EXAMINER

TRAN, ELLEN C

ART UNIT PAPER NUMBER

2134

DATE MAILED: 05/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Advisory Action  
Before the Filing of an Appeal Brief**

Application No.

09/698,159

Applicant(s)

GHOSH ET AL.

Examiner

Ellen C. Tran

Art Unit

2134

**--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

THE REPLY FILED 12 April 2005 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

- a) ☒ The period for reply expires 6 months from the mailing date of the final rejection.  
b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**NOTICE OF APPEAL**

2. ☐ The Notice of Appeal was filed on \_\_\_\_\_. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

**AMENDMENTS**

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because  
(a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);  
(b) ☐ They raise the issue of new matter (see NOTE below);  
(c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or  
(d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: \_\_\_\_\_. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. ☐ Applicant's reply has overcome the following rejection(s): \_\_\_\_\_.

6. ☐ Newly proposed or amended claim(s) \_\_\_\_\_ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.

The status of the claim(s) is (or will be) as follows:

Claim(s) allowed: \_\_\_\_\_.

Claim(s) objected to: \_\_\_\_\_.

Claim(s) rejected: 23-30,33-44 and 47-50.

Claim(s) withdrawn from consideration: \_\_\_\_\_.

**AFFIDAVIT OR OTHER EVIDENCE**

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

**REQUEST FOR RECONSIDERATION/OTHER**

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because:  
See Continuation Sheet

12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08 or PTO-1449) Paper No(s). \_\_\_\_\_

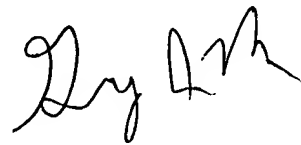
13. ☐ Other: \_\_\_\_\_.

Continuation of 11. does NOT place the application in condition for allowance because: no changes were made to the pending claims to distinguish the claimed invention from the references cited in the rejection. Also no arguments were presented, that would overcome the rejection, see below.

On pages 9-10, the applicant argues that the reference Munson does not teach "neural networks". The Office disagrees "neural networks" as described in the specification on page 8 are defined as: "prior IDSS have employed neural networks to build user profiles based on sequences of commands entered by users". Munson may not use the term "neural networks" but the method is the same as described building user profiles based on sequences of commands entered by the user. Nothing in the claims further distinguishes the term "neural networks" from the meaning provided in applicant's specification on page 8.

On pages 10-11, the applicant argues "application profiles" are not equivalent of the operational profiles utilized by Munson". The Office disagrees, applicant is reminded that the reference as a whole should be considered as teaching the claimed invention. Munson teaches that profiles can be developed based on user input as well as these profiles can be set to an initial standard or further altered based on a users (and system administrators). The applicant further argues that the comparison done in claims 23 and 37 have nothing to do with unconditional probabilities. The Office disagrees a variance is known to be the difference between a point and the average or expected outcome. The fact that the claimed invention is counting and storing a plurality of application data is the same as averaging likewise comparing the difference from this average or expected outcome has the same meaning as variance.

On page 11, the applicant argues that the combination of Munson and Bergman et al. is essentially infeasible. The Office disagrees, Munson does teach "neural networks" claims 33-35 and 47-50 are dependent claims all dealing with a plurality of nodes on the network. Bergman was combined with Munson to shown these "neural networks" could be applied across a plurality of nodes. Bergman takes into account how attacks can be detected on the nodes of a network and propagated downstream to prevent future attacks. It is feasible to combine the two references because it would be an improvement to an intrusion detection system to have a means of determining intrusions based on the similarity of network components.



GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100